API security – limiting factor or accelerator of an open banking strategy?

A whitepaper published jointly by Avaloq and Ergon

avaloq
simplicity for a new era

AIRLOCK®
SECURE ACCESS HUB

avaloq
simplicity for a new era

IT security in the era of open banking

Open banking has become a strategic priority for many financial institutions (FIs) and wealth managers. Local regulation, clients' demand for superior customer experience and the strive for more flexibility are forcing banks to open their platforms to the outside world. In this context, many see IT security as a challenge and an inevitable evil that limits the potential of an ecosystem – but nothing could be further from the truth. When done right, securing APIs is the key factor that drives user experience and defines the potential power of an ecosystem.

Security drives user acceptance and experience

In banking, data privacy and general safety of assets are major concerns for customers. Studies have shown that 49% of bank customers believe that their personal data will be less safe due to open banking.[1] The integration of IT security into an open banking solution is therefore not only a question of securing the planned services - it is an important element that must be transparent to customers and help win their trust. In addition, security is an integral part of their customer experience. While the expectation is to have a seamless and comfortable log-in procedure, the same level of security as one would find in a native mobile banking app must be granted.

Banks begin to connect with the outside

For years, banks have been focused on internal API development. A McKinsey survey conducted in late 2018 revealed that more than 91% of APIs developed by financial institutions were internal.[2]

Just 7% of developed interfaces were partner APIs (mostly encouraged by PSD2 directive) and only 2% represented public APIs.[2]

This is about to change over the next few years, as banks begin to recognize APIs and the participation in ecosystems as a business opportunity, rather than a duty. Or as PwC states it in one of their reports, it is a priority for banks to, "prepare their architecture to connect to anything, anywhere". While tapping into a set of opportunities to future-proof the bank's business model, this openness to ecosystems requires a reimagination of security concepts. The castles have to open their gates and lower their drawbridges, while, at the same time, finding new ways to defend against unwanted guests.

Rising pressure on platform security

As banks and wealth managers go the extra mile to protect their platforms, cyber criminals are stepping up their efforts, too.

Financial institutions reported an increase of 80% of cyberattacks and almost all banks stated that the cybercriminals have become more sophisticated.[3]

In addition, regulators force financial institutions to bear responsibility for correct access management and to guarantee IT security for their clients. This increases the risk of liability for banks and wealth managers. It is, therefore, of paramount importance for any participant in an ecosystem to develop a security framework that ensures the protection of client data, but which also enables future flexibility and the capability to scale.

This whitepaper highlights the external threats to an open banking ecosystem and how to address them. It proposes an effective security framework, sustaining integrity and seamless integration to support a superior customer experience and add to the long-term value of the ecosystem.

Executive summary

A whitepaper published jointly
by Avaloq and Ergon

Key take-aways

1 **IT security in the era of open banking**

Open banking has become a strategic priority for many financial institutions, forcing them to open their platforms up to the outside world. This leads to increased IT security challenges. Done the right way, securing APIs can be a key driver for improved user experiences and a more powerful ecosystem.

2 **A user experience is a security experience**

Security of the past had the unfriendly connotation of a gatekeeper, restricting access and making it difficult for a firm to grow with agility. Today's image is quite different. When implemented well, security processes can serve to tie together what every organization wants: a coherent brand experience, cost-efficient processing, a better conversion rate, and clever user guidance. For banks, key factors to consider are innovation potential, usability, and functionality. Moreover, financial institutions should move towards a coherent security system, with best practices supporting a three-component approach, consisting of a Web Application Firewall, an API Gateway, and Customer Identity and Access Management.

3 **Five security challenges in an open banking ecosystem**

Based on our collective experience in securing open banking ecosystems, Avaloq and Ergon have derived a list of five key security challenges.

- Web Application Firewalls need to upgrade in the face of modern applications that integrate into third-party offerings.
- Traditional XML gateways are not well-suited to the modern type of web services. In the new world of REST and JSON, APIs are used in a fashion that exposes them on the Internet, which places new demands on the API gateway.
- The key reason for using API gateways is access control, including the authorization of clients, user authentication, and consent management, which, in turn, requires further integration with Web Single Sign-on and IAM.
- To be compliant with regulation, such as GDPR and PSD2, identity management and external-user access need to be handled with utmost care, with banks liable for any information misuse.
- When various technologies converge into one, silo thinking in a company can make it difficult to identify who the decision-maker or owner of IT security should be.

4 **Requirements of Open Banking delivered by API security**

We've outlined six key requirements of an open banking ecosystem:

- Protect web applications and APIs to prevent loss of services, data loss and reputational damage.
- Design UI to guarantee an excellent user experience, including onboarding, single sign-on, and adaptive authentication.
- Simplify processes and reduce operational costs via, consolidated security architecture and extensive user self-services.
- Integrate security into the DevOps process, allowing for agile time-to-market.
- Stay flexible to react efficiently to ever-changing compliance regulations.
- Ensure high availability and reliability, in order to avoid long downtimes, even in the case of serious attacks.

A user experience is a security experience

In the worst case, the security of an ecosystem comes in the form of a padlock, mounted to the front door of the system when it has already been built. Done the right way, security by design allows for the combination of standard components like a Web Application Firewall, an API gateway and a Customer Identity & Access Management into an integrated system, guaranteeing a seamless user experience across the whole ecosystem.

The new role of IT security

The fact that security has become intelligent is reflected in our new understanding of IT security manager roles. In the past, the model of a digital security employee was that of a grim gatekeeper, whereas today, he is the friendly concierge and the courteous receptionist. This new image may seem trivial at first glance, but it has concrete consequences, as the example of online portals illustrates.

Let us have a look at the highly competitive market of online shopping. How customers experience onboarding and the check-out process is critical to business success in this industry. After all, whether the conversion succeeds, and the customer completes the desired action, is not only contingent upon the colour of the buttons and the attractiveness of the corporate imagery. Instead, this primarily depends on the user experience that awaits the customer in the authentication and payment process.

Specifically, this means that if shoppers can easily log in for spontaneous digital shopping through social logins and have the system fill out a large part of the delivery and payment information as well, then this is security that becomes a positive user experience. Similarly, if single sign-on enables banking clients to easily use different applications and services, then this is identity management that customers perceive as good service. Intelligent security processes in an ecosystem thus bring together what belongs together: a coherent brand experience, cost-efficient processing, a better conversion rate and clever user guidance.

Defense alone is not enough

In the open banking context, the question is to what extent resources should be invested in IT security – a question that must be answered based on the end goal. This means that IT security as a pure legal requirement is no longer the key point. Instead, the question is: how smart can and must security be today – in terms of high availability, compliance management, cloud solutions, user guidance, convenience and the integration of open banking environments? Every financial institution must ultimately answer this question for themselves, but those who take digitalization seriously will quickly realize that pure defense is no longer enough. The potential for innovation, agility, usability and multifunctionality of the desired solution should be the main decision-making factors.

Coherent security systems instead of point solutions

Whether on-premises or in the cloud, financial institutions must adequately respond to digitization and open banking in terms of security.

There is a clear trend towards an upstream security layer, which offers a series of advantages – namely the convergence of application security, API protection and access management.

More and more applications, APIs, data and identities are being exposed beyond the boundaries of enterprise IT, and Gartner notes: "By 2021, 65 percent of new applications will be built as a system of multichannel applications and multi-layered back-end services that communicate through APIs."[4]

Therefore, integrated systems are required in which individual components are coherently matched and formerly loose ends are reliably linked to one another, even in hybrid cloud environments.

The optimal choice here is a convergent solution consisting of three components:

Web Application Firewall (WAF)
to block attacks on services and applications

API gateway
for the protection of interfaces

Customer Identity & Access Management (IAM)
to control access

The use of these specialised security components to protect exposed interfaces is considered best practice. This assertion applies regardless of whether the specialised security components act at the perimeter of the company network, whether every individual interface is protected by its own security component as a zero-trust architecture, or whether a hybrid approach comes into play.

The OWASP Top 10 of API vulnerabilities

When the topic turns to risks and threats to applications on the Internet, all paths lead to the OWASP Top 10. The Open Web Application Security Project (OWASP) is a non-profit organization and, since 2003, regularly releases a prioritized list of IT vulnerabilities and risks.

The lists of risks and possible countermeasures are based on the data from hundreds of organizations around the globe. OWASP's API security project started to publish a specific Top 10 list on API security in 2019.

While API security was not missing from the well-known previous Top 10 list, with this, OWASP honours the fact that the importance of interfaces, and particularly REST interfaces, has significantly increased, justifying an independent catalogue of threats and measures. The following table shows the full list of API vulnerabilities according to OWASP.[5]

Number	Title	Description
API1	Broken Object Level Authorisation	APIs tend to expose endpoints which process object identifiers, creating a larger area of attack for access controls. Authorisation checks at the object level should be taken into account for every function accessing a data source via user input.
API2	Broken Authentication	Authentication mechanisms are often implemented incorrectly, so attackers can compromise authentication tokens or exploit implementation errors in order to take over the identity of another user temporarily or permanently. If the system's ability to identify the client/user is impaired, API security is impaired as a whole.
API3	Excessive Data Exposure	Considering the very general use of APIs, developers tend to disclose all attributes of objects regardless of individual protection requirements. They rely on clients to filter data before it is shown to the user.
API4	Lack of Resources & Rate Limiting	APIs often contain no restrictions relating to the size or number of resources which can be requested by the client or user. This can affect not only the performance of the API server, leading to denial of service (DoS), but can also keep the door open to authentication faults such as brute force.
API5	Broken Function Level Authorisation	Complex access control guidelines with different hierarchies, groups and roles, as well as an unclear division between administrative and regular functions, tend to lead to authorisation errors. Exploiting these problems gives attackers access to the resources and/or management functions of other users.

Number	Title	Description
API6	Mass Assignment	Linking data provided by the customer (e.g. JSON) to data models without suitable filtering of the properties based on a whitelist generally leads to mass assignment. Guessing object properties, exploring other API endpoints, reading documentation or providing additional object properties in request payloads allows attackers to change object properties that they should not change.
API7	Security Misconfiguration	Errors in security configuration are usually the result of insecure standard configurations, incomplete or ad-hoc configurations, open cloud storage, incorrectly configured HTTP headers, unnecessary HTTP methods, permissive cross-origin resource sharing (CORS) and detailed error messages with sensitive information.
API8	Injection	Injection errors such as SQL, NoSQL, command injection, etc. arise when untrustworthy data is sent to an interpreter as part of a command or a request. The malicious data of the attacker could cause interpreters to execute unintended commands or to access data without the respective authorisation.
API9	Improper Assets Management	APIs tend to publish more end points than traditional web applications, which makes it particularly important to have correct and updated documentation. Correct inventory of hosts and available API versions also plays a key role in reducing problems such as outdated API versions and exposed debug end points.
API10	Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with a lack of or ineffective integration into the risk prevention system, enable attackers to intensify their attacks, nest themselves more deeply and expand their attacks from other systems. All with the aim of manipulating, extracting or destroying data. Most studies show that the time required to detect a breach is over 200 days, and this is usually achieved by external parties rather than internal processes or monitoring.

5 security challenges in an open banking ecosystem

The way web applications communicate in ecosystems has changed fundamentally and requires constant review and adaption of the security framework. Based on Avaloq's and Ergon's combined experience in securing open banking ecosystems, the following list of 5 key security challenges has been derived.

1. **Web application firewalls must learn**

Ten years ago customers still had to be convinced of the benefits of using a Web Application Firewall (WAF). Today, the WAF market is highly competitive and worth billions. Increasing demands on the user experience, as well as an increasing networking of services, are seeing conventional web applications die out. Modern applications are mobile apps or rich clients that run in the browser. Both integrate in-house services and third-party offerings. These services – or APIs – are mostly developed as RESTful web services and use different data formats than those used by traditional web applications. The consequence: protecting these APIs requires new technologies, as the basic interaction paradigm between client and server has changed.

2. **API security is also web security**

Traditional XML gateways are only partially suitable for securing the new type of web services. These are usually designed for SOAP web services that communicate primarily among their peers, require enterprise service buses and are caught in a straitjacket of highly complex standards. This does not fit well with the new world of REST and JSON, which is characterised by agility. In addition, modern APIs are used by a wide variety of clients – from traditional web applications, browser-based rich clients, smartphone apps, "things" and other software systems. As a result, APIs must be exposed on the Internet. This places new demands on the API gateway, similar to those of a WAF, while many of the web security issues of the OWASP Top 10 also become relevant.

3. **APIs need access management**

Content filtering is very important for protecting APIs. The most important reason for the use of API gateways, however, is access control. Access to APIs must be secured using standards such as OAuth 2.0 or OpenID Connect and it is often required to continue to support SAML for access control on existing solutions.

This includes not only the technical authorisation of "clients", but also user authentication and consent management. This, in turn, requires integration with Web Single Sign-on and Customer Identity & Access Management (IAM).

4. **IAM and the customers**

The identities discussed here are very heterogeneous and include a variety of "external" identities, such as those of customers, partners, or systems. These identities need to be managed in accordance with the General Data Protection Regulation (GDPR) in the European Union or the Swiss Federal Act on Data Protection. Failure to adhere to these legal requirements may lead to severe financial penalties. Furthermore, banks in Europe are required to implement the Payment Service Directive 2 (PSD2). With PSD2, banks must provide APIs for account access and payment initiation that enforce strong customer authentication and that may be used by hundreds of so-called third-party providers (TPP). As banks are liable for misuse, access must be tightly controlled. The solution to this complex challenge: customer IAMs (cIAMs), which, unlike enterprise IAM systems, are better at managing external users, as they are easy to scale and guarantee a seamless user experience through integrated onboarding and self-service UIs.

5. **Breaking up inflexible organizational structures**

Another key challenge, however, is less technical, but rather organizational – namely, the silo thinking of many companies. When various technologies converge to form one large whole, who is the contact person and decision maker? Is it the CISO because security issues affect the IT infrastructure and network operations? Or is it the business department, because integrated solutions ensure a lower total cost of ownership and a faster time to market? Or does marketing have to take the lead, because an intuitive user guidance and lower bounce rates are, at the end of the day, the domain of communication and marketing?

Requirements of Open Banking delivered by API security

An ecosystem must come with certain characteristics to fulfill its function as an accelerator of customer experience and a driver of innovation. How security is integrated into the ecosystem has a direct impact on how these requirements perform and are maintained over the long-term. The list below highlights 6 key requirements of an open banking ecosystem and outlines how security contributes to meeting them.

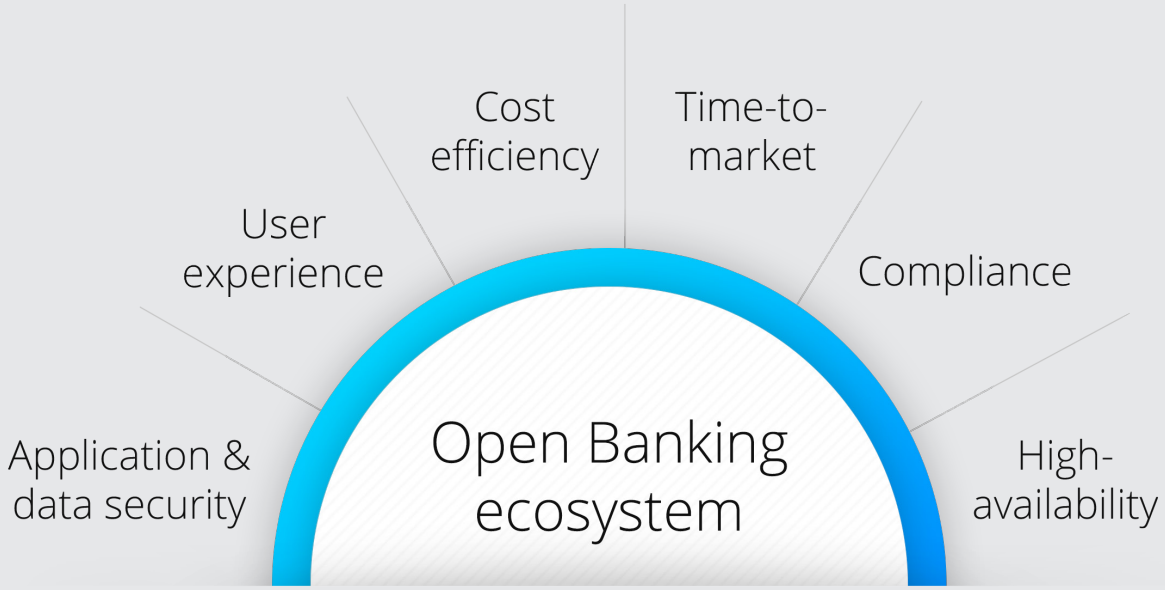
Application and data security

In 2018, attacks at the application level (OWASP Top 10) more than doubled. For this reason, comprehensive protection of web applications and APIs is a business-critical task to prevent loss of services, data loss and reputational damage among customers and partners.

User Experience

When it comes to integrated security solutions, security and user-friendliness are ideally coordinated. Although all user interfaces are based on the principle of 'security first', thanks to extensive user contacts and multiple usability iterations, the user interfaces are designed to guarantee an excellent user experience with simple registration and onboarding processes, extensive user self-services, including consent management, single sign-on, and user-friendly strong authentication, and adaptive authentication.

Figure 1
6 requirements of an open banking ecosystem, defined by the integration of IT security



Cost-efficiency

Simplifying processes and reducing costs – what drives digitalization is also one of the key benefits of an upstream security hub. Integrated security solutions are based on a coherent system architecture and guarantee an attractive TCO. Decoupling of authentication, security and business logic ensures maximum flexibility and a quick time-to-market, while reducing development costs. The consolidated security architecture reduces operational costs, as well. Extensive user self-services result in huge savings for customer services, while increasing user convenience.

Time-to-market

Today, companies need to launch innovative services in ever-shorter cycles. However, as important as speed is, new software solutions must also be secure. This dilemma between security and speed is solved by integrated security services which rely on established and standardised solutions and integrate the security issue into the agile DevOps process. Authentication and security become upfront services in a DevSecOps environment and do not have to be implemented in every application and service. Like this, new applications and services can place their focus on business needs.

Compliance

As regulators are catching up on open banking, compliance for existing and new solutions must address a growing number of policies and global security standards. Regulatory frameworks, like PSD2, MiFID 2 and GDPR in the European Union, demand a certain level of adaptability from financial ecosystems to keep up with their revisions. The same challenge applies to rules for other markets or standards set by the industry, such as the Payment Card Industry Data Security Standard (PCI DSS). A future-proof financial ecosystem has security built in at a central point, where new security requirements can be implemented efficiently and consistently for all applications.

High availability

Account access, payment initiation - when digital services fail, core business activities often fail, too. That's why high availability and a reliability of at least 99.99% is an important security feature to avoid long downtimes, even in the case of serious attacks. Load balancing helps to make services available all the time. Denial-of-service or brute-force attacks can be stopped at a central point and new vulnerabilities (zero-day attacks) can be dealt with quickly, reliably and without impact on the business services.

Make API security the starting point of your open banking journey

API security in an ecosystem is no trivial challenge. It demands the undivided attention of a banking ecosystem's architects and requires significant effort. Currently, the relevant knowledge to design a scalable, future-proof security concept for open banking is owned by a small group of organizations and experts.

The fact that the industry lacks widely distributed and well-established know-how has a restraining effect on the adoption of open banking. On the other hand, a well-designed API security solution has the potential to achieve business value way beyond the simple defensive mechanisms. It can provide important operational functions in an ecosystem, such as the management, authentication and authorisation of tech clients, issuing and validation of API keys or the management and enforcement of usage plans.

Last but not least, the security framework is the key to transparency and traceability in an ecosystem from a compliance perspective, tracking all requests and signing transaction confirmations.

If these fundamental building blocks of API security can be provided centrally for an open banking ecosystem, developers can focus on core functionalities and client experience – enabling the ecosystem to see a real boost in growth.

Contact and authors

Are you interested in learning more about securing open banking ecosystems?
We welcome you to get in touch with one of our API and open banking specialists. See contact information below.

Main contacts and authors

Urs Zurbuchen
Senior Security Consultant
Ergon AG
Email: urs.zurbuchen@ergon.ch

Michael Doujak
Product Manager
Ergon AG
Email: michael.doujak@ergon.ch

Christoph Lutz
Head of Security
Avaloq Evolution AG
Email: christoph.lutz@avaloq.com

Content & editorial
Daniel Studer
Email: daniel.studer@avaloq.com

References

1. PYMNTS.com, Deep Dive: Reducing The Security Risks of Open Banking, available from: https://www.pymnts.com/fraud-prevention/2020/security-risks-open-banking/
2. McKinsey, Next-gen Technology transformation in Financial Services, April 2020
3. Carbon Black, Modern Bank Heists 3.0, May 2020
4. Gartner, Critical Capabilities for Full Life Cycle API Management, 2018
5. OWASP, API Security Top 10 2019, available from: https://owasp.org/www-project-api-security

Avaloq solutions and services

Our solutions and services bring simplicity to financial institutions and wealth managers every day. As a leader in financial software, services and digital technology, we provide the solutions and services financial institutions need to boost efficiencies and foster exceptional relationships.

Avaloq.one Ecosystem

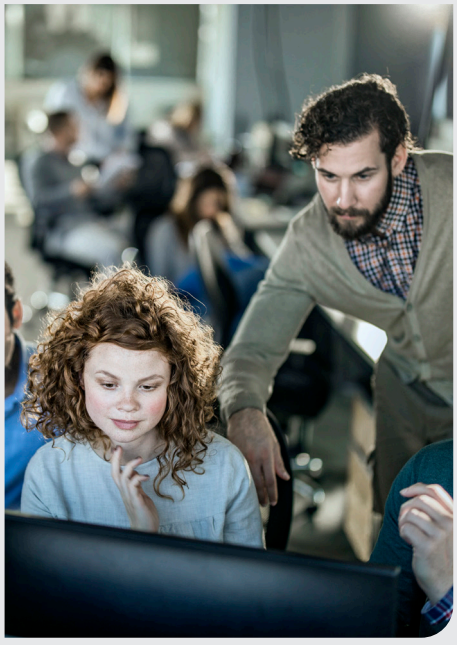
Achieve speed, scale and greater impact

The Avaloq.one Ecosystem brings banks and Fintechs together. We help financial institutions create their own solutions: either using Avaloq sandboxes and APIs or by integrating with fintech solutions available on the Avaloq.one marketplace. Discover the easy way to collaborate and innovate – on one platform.

If you want to learn more about Avaloq.one Ecosystem, visit www.avaloq.one

Avaloq.one benefits:

- Participate in an open, diverse marketplace
- Access to a convenient portal for developers
- Use our cloud sandbox for integration testing
- Take advantage of standardized contracting to procure third-party solutions
- Join our worldwide fintech community of solution providers, banks and investors



Number 1 financial technology and services provider

At Avaloq, we power digital transformation by providing a full end-to-end digital solution, combining our leading technology with a flexible and responsive digital user experience.

We provide financial institutions and wealth managers with the solutions they need to take what is complex and make it simple.

We deliver our powerful digital solutions as SaaS (software as a service), to fully leverage cloud computing, and BPaaS (business process as a service), which lets us automate your services and processes and realize hyper-efficient operations.

Our impact in numbers

150+
clients around the world

CHF 4.5 trillion
client assets managed with Avaloq software

2,000+
Avaloq employees from 66 countries

Visit us at avaloq.com

#avaloqcommunity

avaloq
simplicity for a new era